REMARKS

Applicant thanks the Examiner for examining the application. Claims 1-44 are pending.

Claim Rejections – 35 U.S.C. § 103(a)

The Examiner rejected claims 1-44 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,278,783 to Kocher et al. in view of U.S. Patent No. 7,082,536 to Filip-Martin et al.

Applicant's independent claim 1 requires, among other things, receiving from a first node at an ephemerizer an ephemeral key ID and a message blinded and encrypted with an ephemeral encryption key of an ephemeral key pair to form a blinded and encrypted message, said ephemeral key pair associated with said ephemeral key ID; and decrypting said blinded and encrypted message using an ephemeral decryption key of said ephemeral key pair to form a blinded message. The Examiner cited to col. 2 lines 26-43, col. 6 lines 39-55, col. 7 lines 1-8, col. 4 lines 50-55, and col. 6 lines 65-66 of Kocher et al. as teaching or suggesting these limitations.

However, neither the cited text, nor any other text, of Kocher et al. actually teaches receiving from a first node at an ephemerizer an ephemeral key ID and a message blinded and encrypted with an ephemeral encryption key of an ephemeral key pair to form a blinded and encrypted message, said ephemeral key pair associated with said ephemeral key ID; and decrypting said blinded and encrypted message using an ephemeral decryption key of said ephemeral key pair to form a blinded message, as required by Applicant's independent claim 1.

Kocher et al. is directed towards teaching improvements to implementations of the well-known DES (Data Encryption Standard) cipher, *see at least* col. 2 lines 10-12. These improvements do involve the use of blinded messages, which Kocher et al. does teach are received. However, at no point does Kocher et al. teach or suggest that a blinded message that has also been encrypted with an ephemeral encryption key of an ephemeral key pair, so as to form a blinded and encrypted message, is received, or that such a message is then decrypted, as required by Applicant's independent claim 1. It is

this lack of encryption of the blinded message that distinguishes Kocher et al. from Applicant's independent claim 1.

Indeed, in the portions of Kocher et al. cited by the Examiner, Kocher et al. teaches that an input message M is blinded, *see* col. 2 lines 27-41, but never teaches or suggests that the input message M is encrypted with an ephemeral encryption key of an ephemeral key pair. The same is true for message M and key K as described in col. 6 lines 39-56 of Kocher et al. Kocher et al. teaches how M and K may be divided into M1 and M2, and K1 and K2, respectively, but never requires that M or K is encrypted with an ephemeral encryption key of an ephemeral key pair, *see* col. 6 lines 39-56. Indeed, the purpose of creating these permuted messages (and keys) is to improve the cryptographic process itself, *see at least* col. 6 lines 53-55 ("The permuted keys and messages are then used, rather than the standard key and message, **during the course of cryptographic operations**") (emphasis added), and not to make a message both blinded and encrypted, as required by Applicant's independent claim 1.

This is further shown by the sections of Kocher et al. cited by the Examiner as teaching or suggesting decrypting the encrypted blinded message. In col. 4 lines 50-55, Kocher et al. states:

> The basic DES encryption algorithm uses a 56-bit key to transform a 64-bit plaintext block into a 64-bit ciphertext block. The corresponding decryption operation uses the same key to transform ciphertext blocks into their corresponding plaintexts.

Then, in col. 6 lines 65-66, Kocher et al. states:

> At the end of such operations, the two parts of the ciphertext may be recombined to form the same encrypted/decrypted quantity that would have been produced by a standard DES protocol.

These sentences merely describe DES, and not an actual decryption operation where a blinded and encrypted message is decrypted using an ephemeral decryption key of said ephemeral key pair to form a blinded message, as required by Applicant's independent claim 1. Indeed, the Examiner cannot cite to such language in Kocher et al., because Kocher et al. does not teach or suggest a blinded message that is also encrypted according to an ephemeral encryption key, and then decrypted by using an ephemeral decryption key. Rather, Kocher et al. teaches blinded messages, with no suggestion

that such messages are encrypted or decrypted, that may be used to improve performance of a well-known encryption algorithm, DES.

Therefore, for at least the reasons given above, Kocher et al. does not teach or suggest Applicant's independent claim 1. Thus, Applicant's independent claim 1 is not obvious in light of Kocher et al., and Applicant's independent claim 1 is not obvious in light of Kocher et al. in combination with Filip-Martin et al.

Applicant's independent claims 19, 42, 43, and 44 all include limitations similar to those of Applicant's allowable independent claim 1. Therefore, for at least the reason(s) given above with regards to Applicant's allowable independent claim 1, Applicant's independent claims 19, 42, 43, and 44 are themselves not obvious in light of Kocher et al. in view of Filip-Martin et al., and thus, Applicant's independent claims 19, 42, 43, and 44 are allowable over the combination of Kocher et al. with Filip-Martin et al.

Applicants' dependent claims 2-18 and 20-41 depend from, respectively, Applicants' allowable independent claims 1 and 19. Therefore, for at least the reason(s) given above with regards to Applicants' allowable independent claims 1 and 19, Applicants' dependent claims 2-18 and 20-41 are themselves not obvious in light of Kocher et al. in view of Filip-Martin et al., and thus, Applicants' dependent claims 2-18 and 20-41 are allowable over the combination of Kocher et al. with Filip-Martin et al.

CONCLUSION

Applicant believes this Amendment and Response to be fully responsive to the present Office Action. Thus, based on the foregoing Remarks, Applicant respectfully submits that this application is in condition for allowance. Accordingly, Applicant requests allowance of the application.

Applicant hereby petitions for any extension of time required to maintain the pendency of this case. If there is any fee occasioned by this response that is not paid, please charge any deficiency to Deposit Account No. 50-3735.

Should the enclosed papers or fees be considered incomplete, Applicant respectfully requests that the Patent Office contact the undersigned collect at the telephone number provided below.

Applicant invites the Examiner to contact the Applicant's undersigned Attorney if any issues are deemed to remain prior to allowance.

Respectfully submitted,

Shaun P. Montana, Esq.
Attorney for Applicant(s)
Registration No.: 54,320
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: SUN06-38(P9238)

Dated: April 17, 2007